National School of Cybersecurity
Module: Network Foundation 2

Level: 1st year common core
Prepared by: MA RIAHLA

Lab No. 2: Introduction to the Wireshark (Ethereal) Network Analyzer

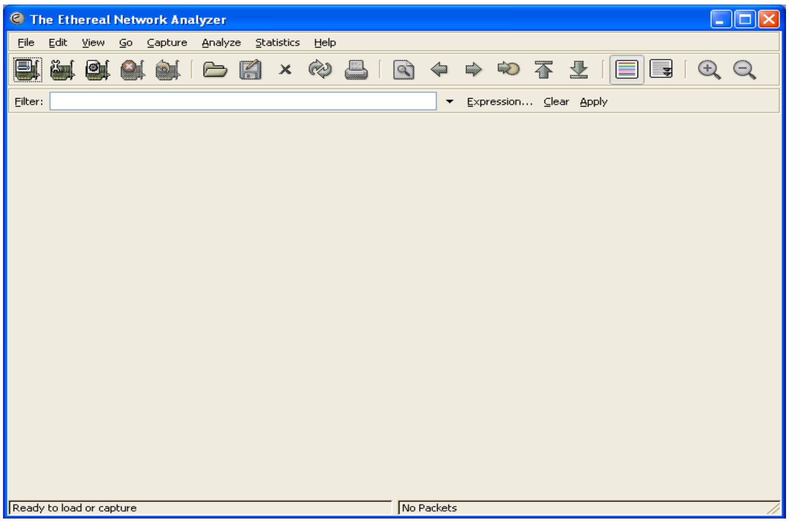
To determine the origin of a network problem, it is often necessary to visualize network traffic (i.e., the packets or frames circulating on the network). These packets must then be analyzed to verify whether the captured traffic conforms to what it should be.

For this purpose, sniffers exist. These are software tools that capture all frames visible to a network interface (regardless of their destination address). Some sniffers also facilitate analysis by decoding part of the traffic, such as displaying the IP and MAC addresses of each frame.

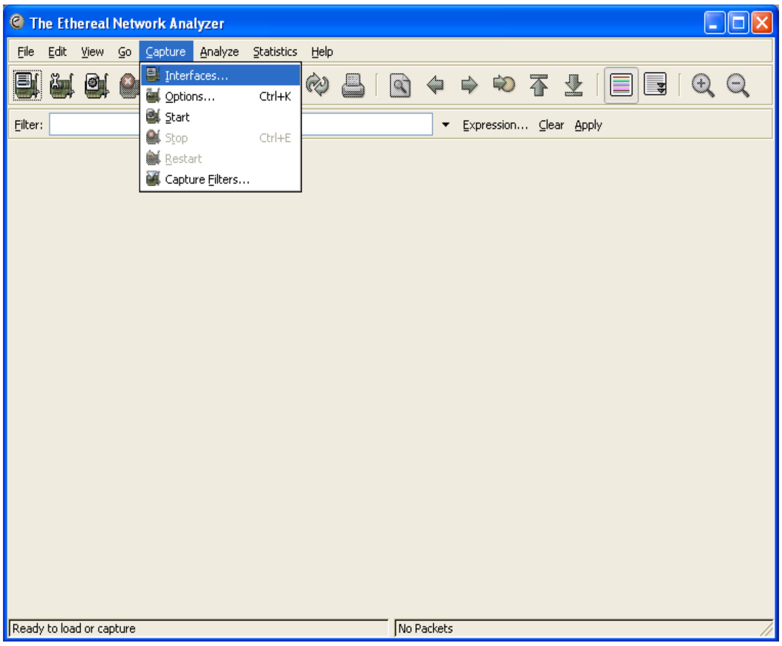
Wireshark is a protocol analyzer. It allows users to examine frames from a file or by capturing them directly from the network.

Moreover, the software includes highly useful features such as capture and display filters and the reconstruction of a TCP session stream. Additionally, the number of protocols recognized by the analyzer is very high."

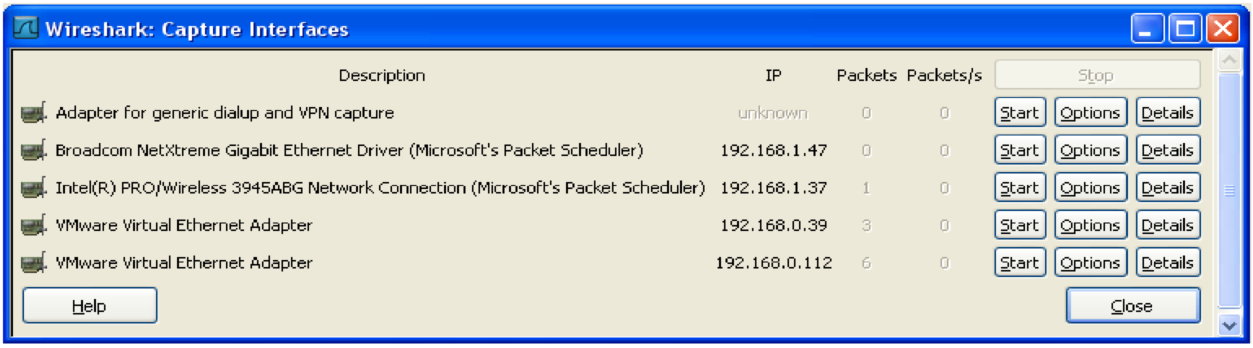
To start the program, click on the '**Wireshark**' icon (on the Desktop). You will see a window like this:


The Ethereal Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Ready to load or capture
No Packets

To start a real-time capture, you need to select an interface (network card) by clicking on '**Capture**' and then '**Interfaces**.' Next, analyze the network by clicking '**Start**' next to the corresponding interface.



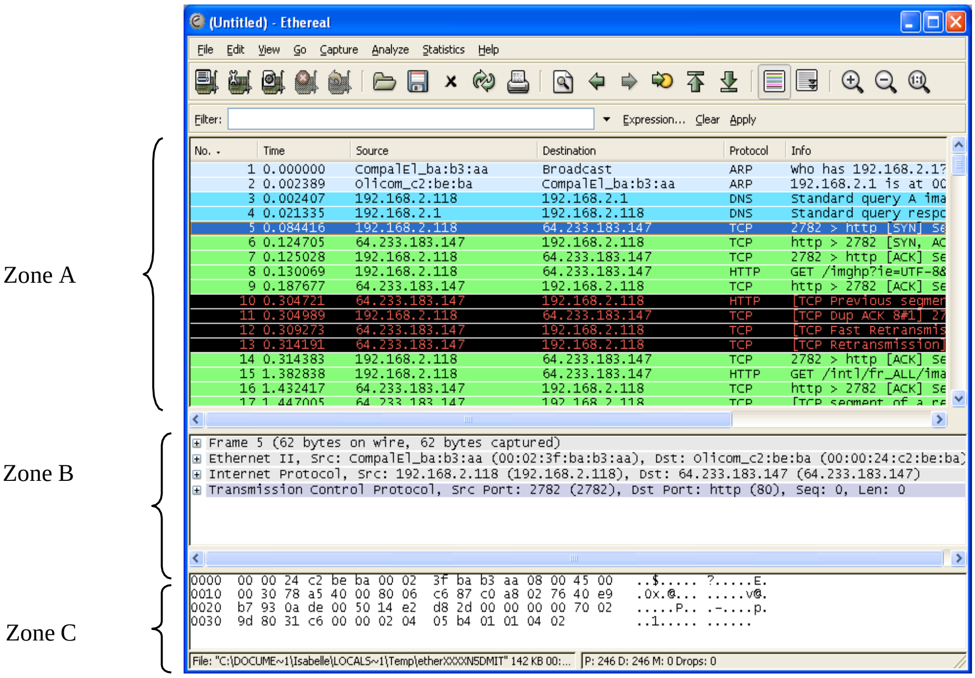
Lab No. 2: Introduction to the Wireshark (Ethereal) Network Analyzer



Wireshark: Capture Interfaces

	Description	IP	Packets	Packets/s	Stop		
	Adapter for generic dialup and VPN capture	unknown	0	0	Start	Options	Details
	Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler)	192.168.1.47	0	0	Start	Options	Details
	Intel(R) PRO/Wireless 3945ABG Network Connection (Microsoft's Packet Scheduler)	192.168.1.37	1	0	Start	Options	Details
	VMware Virtual Ethernet Adapter	192.168.0.39	3	0	Start	Options	Details
	VMware Virtual Ethernet Adapter	192.168.0.112	6	0	Start	Options	Details

You will get a window that looks like this


Zone A
Zone B
Zone C
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time      Source             Destination       Protocol  Info
    1 0.000000  CompalEl_ba:b3:aa  Broadcast         ARP       Who has 192.168.2.1?
    2 0.002389  Olicom_c2:be:ba    CompalEl_ba:b3:aa ARP       192.168.2.1 is at 00
    3 0.002407  192.168.2.118      192.168.2.1       DNS       Standard query A ima
    4 0.021335  192.168.2.1        192.168.2.118     DNS       Standard query respo
    5 0.084416  192.168.2.118      64.233.183.147    TCP       2782 > http [SYN] Se
    6 0.124705  64.233.183.147     192.168.2.118     TCP       http > 2782 [SYN, AC
    7 0.125028  192.168.2.118      64.233.183.147    TCP       2782 > http [ACK] Se
    8 0.130069  192.168.2.118      64.233.183.147    HTTP      GET /imghp?ie=UTF-8&
    9 0.187677  64.233.183.147     192.168.2.118     TCP       http > 2782 [ACK] Se
   10 0.304721  64.233.183.147     192.168.2.118     HTTP      [TCP Previous segmen
   11 0.304989  192.168.2.118      64.233.183.147    TCP       [TCP Dup ACK 8#1] 27
   12 0.309273  64.233.183.147     192.168.2.118     TCP       [TCP Fast Retransmis
   13 0.314191  64.233.183.147     192.168.2.118     TCP       [TCP Retransmission]
   14 0.314383  192.168.2.118      64.233.183.147    TCP       2782 > http [ACK] Se
   15 1.382838  192.168.2.118      64.233.183.147    HTTP      GET /intl/fr_ALL/ima
   16 1.432417  64.233.183.147     192.168.2.118     TCP       http > 2782 [ACK] Se
   17 1.447005  64.233.183.147     192.168.2.118     TCP       [TCP segment of a re
```

```
⊞ Frame 5 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: CompalEl_ba:b3:aa (00:02:3f:ba:b3:aa), Dst: Olicom_c2:be:ba (00:00:24:c2:be:ba)
⊞ Internet Protocol, Src: 192.168.2.118 (192.168.2.118), Dst: 64.233.183.147 (64.233.183.147)
⊞ Transmission Control Protocol, Src Port: 2782 (2782), Dst Port: http (80), Seq: 0, Len: 0
```

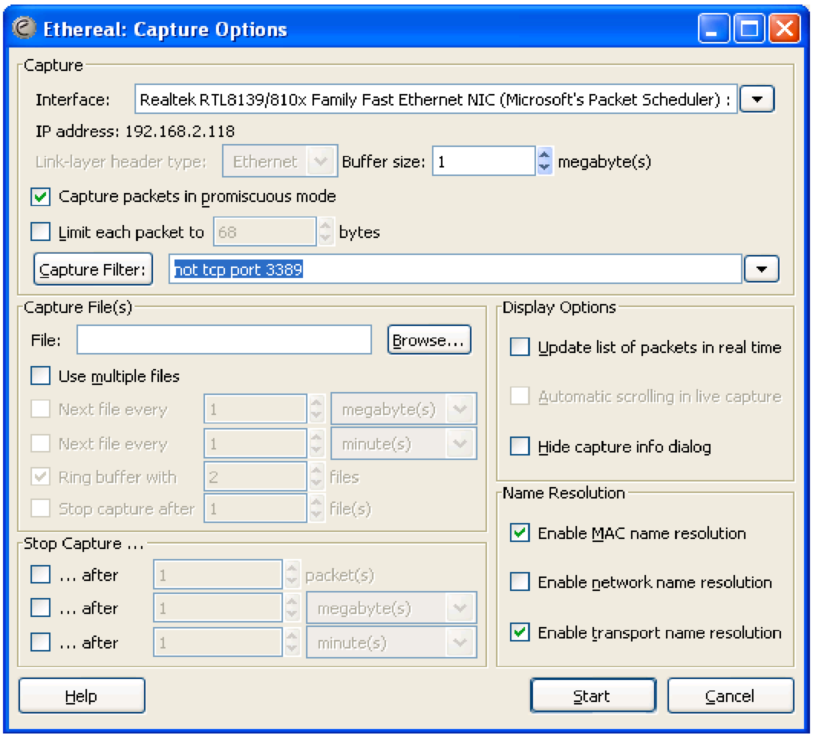
```
0000   00 00 24 c2 be ba 00 02  3f ba b3 aa 08 00 45 00   ..$..... ?.....E.
0010   00 30 78 a5 40 00 80 06  c6 87 c0 a8 02 76 40 e9   .0x.@... .....v@.
0020   b7 93 0a de 00 50 14 e2  d8 2d 00 00 00 00 70 02   .....P.. .-....p.
0030   9d 80 31 c6 00 00 02 04  05 b4 01 01 04 02         ..1..... ......
```

```
File: "C:\DOCUME~1\Isabelle\LOCALS~1\Temp\etherXXXXN5DMIT" 142 KB 00:...   P: 246 D: 246 M: 0 Drops: 0
```

We notice that Wireshark consists of three main panels:

1. This panel displays the list of packets along with their main characteristics. Clicking on this panel controls the display of the other two.
2. The middle panel shows the details of the frame selected in panel 1.
3. The last panel allows you to view the raw content of the frames. It represents the packet selected in panel 1 and highlights the field selected in panel 2.

Now, let's take a closer look at how packets can be captured. After clicking on 'Capture/Options,' you will get the following window:



Ethereal: Capture Options

Capture

Interface: Realtek RTL8139/810x Family Fast Ethernet NIC (Microsoft's Packet Scheduler) :

IP address: 192.168.2.118

Link-layer header type: Ethernet Buffer size: 1 megabyte(s)

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter: not tcp port 3389

Capture File(s)

File: Browse...

□ Use multiple files

□ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

□ Update list of packets in real time

□ Automatic scrolling in live capture

□ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

The capture can be customized with the following settings:

- **Interface:** The network interface on which the capture is performed. Leave the default interface proposed under Windows. For Linux, use ethX, where X is the interface number (usually eth0).
- **Limit each packet to**: Specifies the maximum amount of data to capture for each packet. The default value is usually sufficient for common protocols.
- **Capture packets in promiscuous mode**: The promiscuous option allows capturing packets not intended for us. This is, of course, dependent on the network structure.
- **Capture Filter**: The text box allows you to enter or modify the capture filter. The button opens the dialog box containing the saved filters. The design of a capture filter is presented in the 'Capture Filters' section.
- **File:** This field allows you to specify the name of the file that will be used for the capture when you later choose 'Save' or 'Save as...' in the 'File' menu of Ethereal.
- **Capture limits**: It is possible to stop the capture based on different criteria: number of packets, kilobytes, or seconds.
- **Enable MAC name resolution**: Allows translating the first three bytes of MAC addresses into the manufacturer's name.
- **Enable network name resolution**: Allows translating IP addresses into the corresponding machine name.
- **Enable transport name resolution**: Allows displaying the protocol name for known port numbers.

When all the options are selected, click on '**Start**' to begin a new capture. Click on the '**Stop**' button to end the capture session.

The display can be modified as desired using the display filters, which we will discuss later.

Lab No. 2: Introduction to the Wireshark (Ethereal) Network Analyzer

Capture Filters

Ethereal uses capture filters based on the libpcap language. The complete syntax is explained in the tcpdump manual (man tcpdump on Unix/Linux). Capture filters are specified in the capture options dialog. It is possible to store different filters. To do this, you need to open the capture filter editing dialog by clicking on the '**Capture**' menu / '**Capture Filters**...'. This dialog can also be displayed from the capture options using the **'Capture Filter**' button.

Example

The two filters below are equivalent: capturing HTTP traffic.
(src port 80) or (dst port 80) or port 80.

- ***Saving Captures***

It is possible to save captures to import them into a number of protocol analyzers. To do this, click on **File**/**Save as** and then save after giving a name to the capture.

- ***Display Filters***

After performing a capture, it is always possible to modify the packet display by specifying a display filter (or post-capture filter).

Display filters offer a significantly larger number of options and recognized protocols compared to capture filters. The selection can be made based on:

- A protocol.
- The presence of a field.
- The values of fields.
- The comparison of fields.

Display filters are written in the text box at the top of the Ethereal window (or by clicking on Analyze/display filters).

Practical Exercise

Try to ping (ping 192.168.0.2) and capture the various information discussed earlier. The protocol used for pings is ICMP.